

Resources for INFOSEC Educators

FISSEA March 2000 Conference

Wednesday March 15, 2000

M. E. Kabay, PhD, CISSP

Security Leader, INFOSEC Group

AtomicTangerine, Inc.

mkabay@compuserve.com

at@mictangerine.

Contact information

M. E. Kabay, PhD, CISSP
can be reached at
255 Flood Road
Barre, VT 05641-4060
V: +1.802.479.7937
F: +1.802.479.1879
E: mkabay@compuserve.com

- AtomicTangerine is the Internet's first e-business venture consulting firm, combining the disciplines of venture capital, technology innovation and strategic consulting to create category killers and incubate new industries for companies of all sizes and at all stages of evolution. AtomicTangerine headquarters are in the San Francisco Bay Area and we have offices in New York, London, Tokyo, Washington DC, Boston, Denver and Seattle/Tacoma. Visit our new Web site at <www.atomictangerine.com>.

at@mictangerine.

Goals

- Make sure INFOSEC educators are not missing basic resources for newsletters and courses
- NOT covering technical vulnerabilities
- Provide excerpts from free, useful e-publications
- Point to archives of materials useful for newsletters and courses

at@mictangerine.

Overview

- RISKS Digest
- SANS Newsbites
- ComputerCrime Alert
- Network World Security Newsletter
- SecurityPortal
- NewsScan
- EDUPAGE
- EntryPoint
- Information Security Magazine
- Web sites
- INFOSEC Educators List
- MK documents

at@mictangerine.

RISKS-LIST: Risks-Forum Digest Monday 28 February 2000 Volume 20 : Issue 82
FORUM ON RISKS TO THE PUBLIC IN COMPUTERS AND RELATED SYSTEMS (comp.risks)
ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator
***** See last item for further information, disclaimers, caveats, etc. *****
This issue is archived at <URL:<http://catless.ncl.ac.uk/Risks/20.82.html>>
and by anonymous ftp at ftp.sri.com, cd risks .

Contents:

U.S. government abandons Bernstein restrictions (Jeremy Epstein)
How to make friends, influence hackers, and build bugfree code Paris style (Peter Wayner)
Someone making sense about e-commerce (Paul Robinson)
The Millennium Bug Revisited (R A Downes)
It was just a network board... (Debora Weber-Wulff)
Risks of National Weather Service tests (John O Long)
Re: Microsoft responds (R A Downes)
Re: Great West gives out too much personal info (Taylor Hutt, Bob Hofkin)
Imbalanced parentheses or angle brackets (W.T. Shymanski)
"Unstable" postal addresses (Joseph A. Dellinger)
REVIEW: "Security Technologies for the World Wide Web", Rolf Oppliger (Rob Slade)
Abridged info on RISKS (comp.risks)

at@mictangerine.

RISKS Digest

- Newsgroup and e-mail
 - security holes, breaches, quality-assurance failures, discussions of fundamental issues
- Highly-regarded
 - Moderated by Peter G Neumann, PhD
- Irregular publication schedule for DIGEST
- Archives going back decades
 - <http://catless.ncl.ac.uk/Risks/vv.nn.html>
- For full info see
<http://www.CSL.sri.com/risksinfo.html>

at@mictangerine.

SANS NEWSBITES — The SANS Weekly Security News Overview
Volume 2, Number 9 — March 2, 2000 <sansro@sans.org>
Editorial Team: Kathy Bradford, Crispin Cowan, Roland Grefer, Rob Kolstad,
Bill Murray, Stephen Norhcutt, Alan Paller, Howard Schmidt, Eugene
Schultz

25-02-2000 The Week in Review
28-02-2000 Universities to Receive SSH Free
26-02-2000 Bernstein May Post Encryption Code
26-02-2000 FBI Web Site Attacked
25-02-2000 Vandals May Use Windows for Future DDoS Attacks
25-02-2000 Microsoft Security Issues
25-02-2000 Have Attack Defense Strategies in Place, Say Expert
24-02-2000 Microsoft Fights Off "Synflood" Attack
24-02-2000 First Windows 2000 Virus: W2K.Infis.4608
24-02-2000 Computer Science Student Charged as Cracker
24-02-2000 ActiveX Security Hole
24-02-2000 NDB.com Suffers Attack, Outage
24-02-2000 CIA Says Cyber Threat from Russia and China is Developing
24-02-2000 ICQ Account Hijacked; Ransom Demanded
23-02-2000 ISPs Form Alliance to Fight DDoS Attacks
23-02-2000 Israeli Legislator Reconsiders Position on Hacker Conference
23-02-2000 Canadian Government Sites Hacked
22-02-2000 Net Healthcare Ethics
21-02-2000 Always On Connections Vulnerable to Infiltration
21-02-2000 Cyber Attacks on US Government Systems Prevalent
21-02-2000 Internet Security Holes
15-02-2000 Cyber Crime on the Rise in the UK
15-02-2000 Virginia DMV Web Site Attacked

at@mictangerine.

SANS NewsBites

- System Administration and Network Security organization
- Summarize key developments, provide hyperlinks
- For a free subscription, e-mail sans@sans.org with the subject: **Subscribe NewsBites**

at@mictangerine.

From: alerts@theMezz.com
Hacker 'Gatsby' Gets 18-Month Sentence
7.19 a.m. ET (1219 GMT) March 5, 2000
SAN DIEGO — A computer hacker known online as "The Gatsby" will spend 18 months in federal prison.
A judge in San Diego has sentenced Jonathan Bosanac for electronically breaking into some of the country's largest computer systems.
The judge said his wrongdoing caused more than \$1 million in damage to one company alone.
Bosanac was ordered to pay \$10,000 in restitution to three telephone companies he hacked into.
He pleaded guilty in December to participating in one of the nation's biggest hacking schemes.
The crimes took place more than five years ago. Friends say the man's life has since turned around. He's been working as a computer consultant.

Get your own subscription here:
<http://theMezz.com/alerts>

at@mictangerine.

ComputerCrime-Alert

- Joe Mezzanini
- 1-5 news articles / day
- No commentary
- Useful case studies
- Go to Web site to subscribe:
<http://theMezz.com/alerts>

at@mictangerine.

NETWORK WORLD FUSION FOCUS:
M. E. KABAY on SECURITY
Today's Focus: Ignorance or Lies — 03/07/00
Kevin Mitnick published a letter in The Guardian newspaper and perhaps others on Feb. 22. Today I want to focus on one question in his letter: "What threat did I present when I hacked into Sun's computers?"
Criminal hackers and their supporters often use this flawed defense as an excuse after breaking into other people's systems without permission. They seem to think that as long as they don't modify information, they haven't done anything wrong. Some of them say information should be free, and imply there is something wrong with confidentiality, especially confidentiality of corporate communications and documents.
I suspect that most of the people who excuse unauthorized access to computers and networks have never worked with production systems. A production system is one whose functions are essential for the operations of its owners. For example, a real-time process-control computer in a factory is a production system; so are the computer and the network underlying a hospital registration system.
....

at@mictangerine.

Network World Security Newsletter

- MK began writing Feb 2000
- Short articles (400-1000 words)
- Non-technical issues in INFOSEC
- Designed to be useful for awareness programs
- Provoking interesting responses from readers
- Responsive to requests — let me know what you'd be interested in reading about
- Go to Web site for information on subscriptions:
– <http://www.nwfusion.com/newsletters/sec/>

at@mictangerine.

SecurityPortal.com 13 March 2000
The Future of Computer Crime: It Ain't Just Hacking
What did you think of famed hacker Kevin Mitnick's testimony before a U.S. Senate committee? Ron Mendell followed the testimony, and has some interesting insights on the future of e-crime.
'In actuality, Mitnick, "Coolio," alleged master hacker, and others simply may be some guy behind a curtain, albeit an electronic one, pretending to be the Wizard of Oz in cyberspace. And, Mitnick (and his acolytes) never laid claim to designing a new computer language or operating system or contributing to the solution of Fermat's Last Theorem. Rather, his confessed tricks are those of the charlatan, the "carny con artist," the social engineer. He knows the psychological Achilles' heel of virtual space.' Read it all here.
<<http://securityportal.com/direct.cgi?/cover/coverstory20000313.html>>
***** Vendor Corner *****
New from SANS
***** Top News *****
Recent postings in our top news
<<http://www.securityportal.com/framestetopnews.html>>

SecurityPortal

- Weekly e-pub
- Jim Reavis — short editorials and comment
- Paragraph-long summaries of news items
- Hyperlinks to full stories
- To subscribe, visit Web site

NewsScan Daily, 9 March 2000 ("Above The Fold")

"ABOVE THE FOLD"
Net Execs Look To "Post-PC World"
Qwest Is Coy Over Mystery Suitor
Estee Lauder Wins Suit Over Trademarked "Keywords"
Oracle Teams With Wal-Mart, Chevron In B2b Network
Report Raises Online Privacy Concerns
Unbreakable Hyperlinks
Movie Tickets On The Web

FEATURES
Flash Card
Mailbag: Lawyer Talk, Pirate Songs, & Out-of-the-Box Thinking
....

NewsScan

- John Gehl & Suzanne Douglas
 - Former editors of EDUPAGE
 - Editors of INNOVATION
- Entire field of information technology
 - strong interest in security stories
- Superb one-paragraph summaries
- Hypertext links to full stories
- Subscriptions (free):
e-mail to NewsScan@NewsScan.com
with subject = subscribe
- Bonus: various interesting topics at end (biographies, quotations. . . .)

Edupage is a service of EDUCAUSE, an international nonprofit association dedicated to transforming education through information technologies.

TOP STORIES for March 6, 2000
Mailing Supplier and IBM Try Postage Sales on Net
First 'Digital Divide' Bill Passes Senate
Clinton Sees Chances as Good for Online Privacy Bill This Year
Net Spending Decisions Reflect Customer Is King

ALSO
Internet Providers Look for Profit in Free Access
A Virtual Revolution in Teaching
Time Running Out on Kid E-mail
Napster Is Rocking the Music Industry
....

EDUPAGE

- Similar to NewsScan
- 3 times a week
- Longer abstracts, fewer items
- No hypertext links
- To SUBSCRIBE to Edupage,
send an e-mail message to
LISTSERV@LISTSERV.EDUCAUSE.EDU
and in the body of the message type:
SUBSCRIBE Edupage *YourFirstName YourLastName*



EntryPoint

- Successor to PointCast News
 - Web-scan engine
 - Personalized portal
- Provides titles and URLs for hypertext links
- Does not download full story in advance
- Multiple “channels”
- Alerts
 - configure a few key words (limited)
 - define action (change color of NEWS icon, show headlines)
- Go to <http://www.entrypoint.com> for info, software



Information Security Magazine

- [Http://www.infosecuritymag.com](http://www.infosecuritymag.com)
- Monthly free magazine
 - top writers such as Donn Parker, Bruce Schneier
 - in-depth articles of direct use for awareness & training
- SecurityWire Daily on Web site
 - 4-6 top stories with hypertext links
 - available by e-mail
 - <http://www.infosecuritymag.com/securitywire/index.html>

Web Sites

- Multitude of good resources
- Some key starting points:
- CERIAS Security Hotlist
<http://www.cerias.purdue.edu/>
- Data Security Sources <http://www.dso.com/>
- Dr Dobbs Computer Security
<http://www.ddj.com/topics/security/>
- ICSA.net <http://www.icsa.net>
- Information Security Resources - Current Online Publications
<http://security.isu.edu/publications.html>

Web Sites (cont'd)

- NIST Computer Security Resource Clearinghouse <http://csrc.nist.gov/>
- SecurityPortal.com
<http://www.securityportal.com/>
- TSCM - Counterintelligence and Technical Security Links
<http://www.tscm.com/intelsites.html>
- Unified INFOSEC Glossary
<http://security.isu.edu/glossary.html>
- Web Security Pointers
<http://www.security.mci.net/web-security.html>

[secedu] Digest Number 53

Community email addresses:

Post message: secedu@onelist.com
Subscribe: secedu-subscribe@onelist.com
Unsubscribe: secedu-unsubscribe@onelist.com
List owner: secedu-owner@onelist.com

Shortcut URL to this page:

<http://www.onelist.com/community/secedu>

There is 1 message in this issue.

Topics in today's digest:

1. REVIEW: "Intrusion Detection", Rebecca Gurley Bace
From: "Rob Slade, doting grandpa of Ryan and Trevor" <rslade@sprint.ca>

....

at@mic tangerine.

INFOSEC Educators List

- Discussion/distribution list run by Dr Fred Cohen
- Open to questions from participants
- Conference RFPs, announcements
- Book reviews
- Pointers to articles of interest
- Postings of occasional articles

at@mic tangerine.

MK Documents — IYIR

- INFOSEC YEAR IN REVIEW
 - ~500 abstracts/year about issues in INFOSEC
- Topic areas
 - Computer crimes
 - Emerging vulnerabilities
 - Management & policy
 - Cryptography, law & e-commerce

at@mic tangerine.

MK Documents — IYIR (Cont'd)

- Reports freely available / usable
 - <http://www.isc2.org/iyir1996.pdf>
 - <http://www.isc2.org/iyir1997.pdf>
 - <http://www.isc2.org/iyir1998.pdf>
 - http://www.icsa.net/html/library/whitepapers/infosec/InfoSec_Year_in_Review_1999-mm.pdf where mm refers to month (01=Jan, etc.)
 - 1999 edition nearly done

at@mic tangerine.

MK Documents — PowerPoint Archives

- Organizing all INFOSEC UPDATE course materials by topic to post on ADARIO Web site (<http://www.adario.com>)
- E.g.,
 - 11 Breaches of confidentiality
 - 12 Wiretapping, interception (not jamming)
 - 13 Data diddling/corruption, embezzlement
 - 14 Viruses, Trojans, hoaxes
 - 15 Fraud (not embezzlement), extortion
 - 16 INFOWAR, industrial espionage
 - 17 Penetration, phreaking. . . .
- Expect announcement in INFOSEC Educators List, RISKS, etc.

at@mic tangerine.

Outreach

- Criminal hacker propaganda swallowed by news media
- Criminal hackers and their supporters appearing before Congress and in government
- Children fooled into accepting lies about "harmless" intrusions
- Need to oppose trend by telling truth about effects of unauthorized penetration and denial of service attacks
- Everyone in this room has something to contribute to public evolution of INFOSEC knowledge
- Schools, clubs, churches, mosques, synagogues. . . .
- Two papers to start you off!

at@mic tangerine.

